Amendments to the Specification:

Please replace the paragraph on page 8, lines 3 to 21, with the following rewritten paragraph:

Referring now to the drawings, and more particularly to Figure 1, there is shown a high level diagram showing a means for denying access to data according to the present invention. In the preferred embodiment of the present invention a helicopter includes two removable, rugged commercial mass memory devices. These devices communicate, via small computer system interface (SCSI) bus 101, with a mission computer (MC) 102 and a flight management computer (FMC) 103. The FMC typically performs flight related and unclassified tasks; however, in the preferred embodiment the FMC may be reconfigured to perform some of the tasks normally performed by the MC. The MC typically performs mission-specific tasks which by their nature are often classified. One mass memory device is a disk drive (EMSU) 104, and the other is a dual PCMCIA card reader (DTS) 105 which uses flash memory cards. The EMSU 104 and each of the flash memory cards appear to the computers as disks, with the EMSU and one flash memory card each ~~contain~~ containing a large amount of data. Different sets of data may be classified or unclassified. The other flash memory card generally contains only unclassified data. It would be apparent to one skilled in the art that various media type may be used and the present invention is not limited to EMSU and DTS devices.

Please replace the paragraph starting on page 8, lines 22 to 29, and continuing on page 9, lines 1 to 11 with the following rewritten paragraph:

In the preferred embodiment, the encryption function in the MC is performed by an encrypting SCSI device driver in the operating system. This device driver either passes the SCSI data through untouched or applies encryption

or decryption to the data as needed. Encrypted data on the EMSU or DTS is identified by an encryption flag in the file header. If the flag is present for data read from the DTS or EMSU, then the data ~~needs~~ need to be decrypted and is routed through the decryption algorithm before being handed to the calling application. If no flag is present, then the data is unclassified plain text and is passed straight to the calling application. Classified data to be written to a storage medium 104 or 105 is delivered to the encrypting SCSI device driver in the MC where it is encrypted and transferred to ~~wither~~ either the EMSU 104 or the DTS 105. It would be apparent to one skilled in the art that various algorithms for encryption may be used, and that a hardware encryptor/decryptor could be substituted for the SCSI device driver. A substitute algorithm would be selected by weighing factors related to ease of use/integration, robustness, and the algorithm's inherent ability to withstand cracking; thus, the present invention is not limited to any one encryption/decryption algorithm or limited only to software implementation.